Présentation

Objectifs

L'essor d'Internet a incontestablement accéléré et facilité les accès et les échanges de l'information. Cette fulgurante réussite dans la communication a favorisé l'apparition de nouvelles menaces criminelles. Ces menaces font courir des risques considérables pour les entreprises, les administrations publiques et les particuliers. La lutte contre la cybercriminalité est devenue un défi majeur mondial en raison de la dimension internationale de cette nouvelle délinquance souvent organisée.

La cybercriminalité évolue chaque jour, faisant apparaître de nouvelles formes de risques et de techniques de contournement de la loi, que le droit se doit de prendre en considération et auxquelles il doit s'adapter.

Le principal objectif de cette formation pluridisciplinaire est d'appréhender les différentes infractions et responsabilités liées à l'utilisation frauduleuse des réseaux numériques et des systèmes d'information..

Elle apporte aux acteurs économiques, aux responsables des systèmes d'information, aux professionnels du droit, aux forces de l'ordre et à toutes les personnes confrontées à la sécurité numérique un éclairage sur :

- la nature des menaces liées aux réseaux numériques.
- Les dispositifs juridiques de lutte contre la cybercriminalité.
- les techniques d'investigation numérique et les procédures d'établissement de la preuve.
- les questions et les réponses juridiques qui se mettent en place aux plans national, européen et mondial

Diplôme soutenu par l'Ecole Nationale de la Magistrature

Programme

UE1: Introductions aux réseaux et à l'Internet

(Mise à niveau technique)

- Organisation et structure physique des réseaux informatiques
- Caractéristiques techniques du réseau Internet (TCP/IP, DNS, WiFi, Routage IP, LAN, WAN.)
- Caractéristiques des nouveaux services et modes de développement du numérique (Web2.0, 3.0 et 4.0, BigData, Objets connectés et IoT, cloud computing, développement AGILE.).
- Certificats et protocoles (SSL, Https, ..)
- Clear Web, Deep Web, Dark Web: caractéristiques et modes opératoires
- Les fournisseurs de services de la société de l'information: rôles, et qualification juridique.

UE2: Introduction au Droit et à la sécurité juridique

(Mise à niveau juridique)

- Les différentes branches du droit
- Introduction au Droit pénal et aux principes directeurs du procès pénal
- Introduction à la propriété intellectuelle et ses incidences dans l'univers numérique

UE3: Introduction aux aspects techniques de la sécurité des systèmes d'information et de la cybercriminalité

- Système d'information: définition, rôle, techniques d'intrusion et critères d'évaluation d'un SI
- Cybercriminalité: menaces, piratage informatique, usurpation d'identité, e-réputation, Social engineering, APT, interception des données, blocage de systèmes, attaque DDoS, attaque par Force brute, Phishing, Ransomware, Backdoors, Vulnérabilités - Cas pratiques
- Introduction à la signature électronique et à la cryptologie (techniques de base de codage des données)
- Principaux dispositifs et règles de prévention et de protection des systèmes d'information

UE4: Cybercriminalité: aspects juridiques, enjeux économiques et sociaux et coopération internationale

- Les obligations légales et réglementaires de sécurisation des systèmes d'information
- Les aspects juridiques de la démarche de sécurisation (cryptologie, chartes, préservation de la preuve, signalement des incidents...)
- Aspects techniques, juridiques et réglementaires de la dématérialisation des échanges
- Sécurité de l'information et intelligence économique
- Instances de régulation, de prévention et de répression
- Droits et obligations des acteurs de la société de l'information
- Introduction aux monnaies virtuelles et aux crypto-monnaies (Bitcoin, Blockchain, ...): caractéristiques, enjeux et risques.
- Menaces et qualification juridique (évolutions législatives et dispositions pénales)
- Lutte contre la cybercriminalité et Libertés et Droits fondamentaux
- Enjeux, et défis de la protection des données personnelles (décryptage du règlement européen)
- Impact économique, sanitaire, social de la cybercriminalité (blanchiment d'argent, cyberfraudes, contrefaçon..)
- Réseaux sociaux: impacts pour l'entreprise, risques et responsabilités
- Méthodes d'anticipation des risques et des sanctions pénales
- Stratégies (nationale et internationale) de lutte contre la cybercriminalité et coopération internationale

UE5: Investigation et Informatique légale

- Défis et contexte de l'investigation numérique (criminalistique et investigation cybercriminelle)
- Présentation des principales méthodes d'investigation (analyse des traces internet, analyse des supports (disques, smartphone...)
- Interception des données sur le réseau Internet, live forensic, infiltrations, enquête sous pseudonyme, captation de données: pratiques et encadrement juridique
- Critères d'admission de la preuve électronique
- Cadre juridique et mission et déroulement de l'expertise
- Préparation d'un rapport d'expertise forensic

CONDITIONS D'ADMISSION

Formation initiale

Etudiants ayant validé une licence obtenue dans une université de l'espace européen ou un diplôme équivalent.

Formation continue

Cette formation s'adresse aux professionnels souhaitant développer des compétences dans le domaine de la lutte contre la cybercriminalité et la sûreté numérique. Elle permet de comprendre les enjeux de la sécurité de l'information et de la cybercriminalité, et d'en maîtriser les aspects juridiques.

Les professionnels peuvent ainsi valoriser l'expérience professionnelle qu'ils ont acquise, par l'obtention d'un diplôme universitaire.

Exemples de professionnels concernés par cette formation :

- Les professionnels du droit (Magistrats, Avocats, Juristes spécialisés, ..)
- Les fonctionnaires travaillant dans les différents Ministères (Justice, Défense, Intérieur, Economie numérique, ..) et intéressés par l'acquisition de compétences dans le domaine de la lutte contre la Cybercriminalité
- les salariés de l'industrie ou des collectivités locales (DSI, RSSI, Ingénieurs, ..)
- Le personnel chargé des enquêtes ou de leur supervision dans les affaires de criminalité informatique

Pré-requis : des connaissances de base (bureautique) sur les ordinateurs et sur Internet sont fortement conseillées. Un programme de mise à niveau informatique est prévu, de même qu'un programme de mise à niveau juridique pour les étudiants et les professionnels non juristes.

La mise à niveau se déroule lors du premier mois de la formation (Janvier).

CONDITIONS D'INSCRIPTION :

- **Sélection sur dossier**
- **Date limite** de dépôt des dossiers de candidature: **8 janvier 2017**
- **Capacité d'accueil limitée (20)**

Droits d'inscription :

- Professionnels: **1500 €**
- Etudiants: **400 €**

Calendrier universitaire:

- Volume horaire **: 130h**
- Début des cours: **11 Janvier 2016**
- Fin des cours **: 7 juillet 2017**
- Rythme des cours **: 2,5 jours par mois**
- Lieu: **Faculté de Droit et science politique de Montpellier**

RENSEIGNEMENTS ET RETRAIT DE DOSSIER

Secrétariat CRESIC
Adresse: 14, rue Cardinal de Cabrières
34060 MONTPELLIER CEDEX
Tél: 04 34 43 29 53
Courriel: du-cybercrime@umontpellier.fr
Site: http://cybercrime.edu.univ-montpellier.fr

OU

Service Formation continue-Université de Montpellier

Adresse: Espace Richter, Rue Vendémiaire, Bât. E - CS 29555 34961 Montpellier, cedex 2
Tél : 04 34 43 21 21-Fax : 04 34 43 21 90
Courriel: sfc@umontpellier.fr

DIPLÔME D'UNIVERSITÉ

Cybercriminalité

Droit, Sécurité de l'information et Investigation numérique légale

Directeur: **Adel Jomni**

- **Enseignant-chercheur (Université de Montpellier)**
- **Expert auprès du Conseil de l'Europe**
- **Membre de European Cybercrime Training & Education Group (ECTEG)**
- **Directeur du CRESIC (Centre de Recherche et d'Etude sur la Sécurité de l'Information et la Cybercriminalité)**